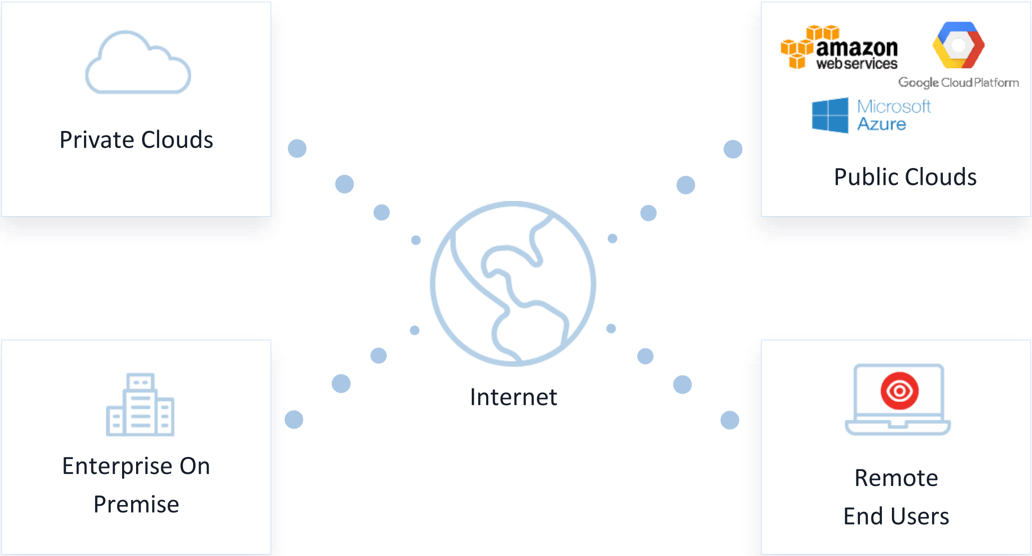
QSC19

Qualys Security Conference Dubai

Cloud Agent Platform Overview

Chris Carlson
VP, Product Management, Qualys, Inc.

Digital Transformation is Driving IT Transformation for Organizations



Private Clouds

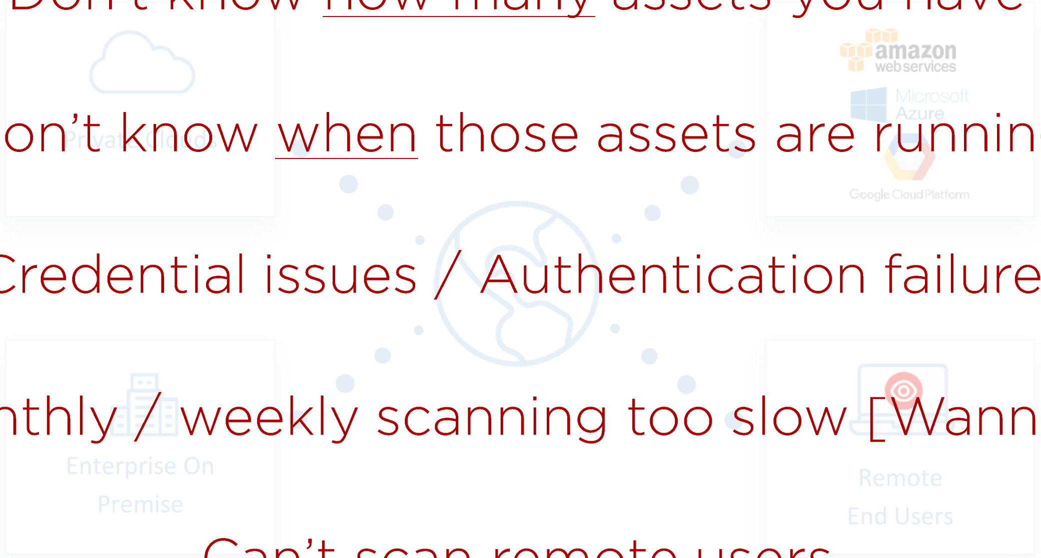
Public Clouds

Internet

Enterprise On Premise

Remote End Users

… But creates new Challenges for Security



Don’t know how many assets you have

Don’t know when those assets are running

Credential issues / Authentication failures

Monthly / weekly scanning too slow [WannaCry]

Can’t scan remote users

Qualys Sensors

Scalable, self-updating & centrally managed

Physical

Legacy data centers

Corporate infrastructure

Continuous security and compliance scanning

Virtual

Private cloud infrastructure

Virtualized Infrastructure

Continuous security and compliance scanning

Cloud/Container

Commercial IaaS & PaaS clouds

Pre-certified in market place

Fully automated with API orchestration

Continuous security and compliance scanning

Cloud Agents

Light weight, multi-platform

On premise, elastic cloud & endpoints

Real-time data collection

Continuous evaluation on platform for security and compliance

Passive

Passively sniff on network

Real-time device discovery & identification

Identification of APT network traffic

Extract malware files from network for analysis

API

Integration with Threat Intel feeds

CMDB Integration

Log connectors

Qualys Cloud Agent Platform

Lightweight
Software Agent

(collects metadata only)

On-Premise
Servers

Public Cloud

User
Endpoints

Windows

Linux

Mac

AIX

Cloud Native

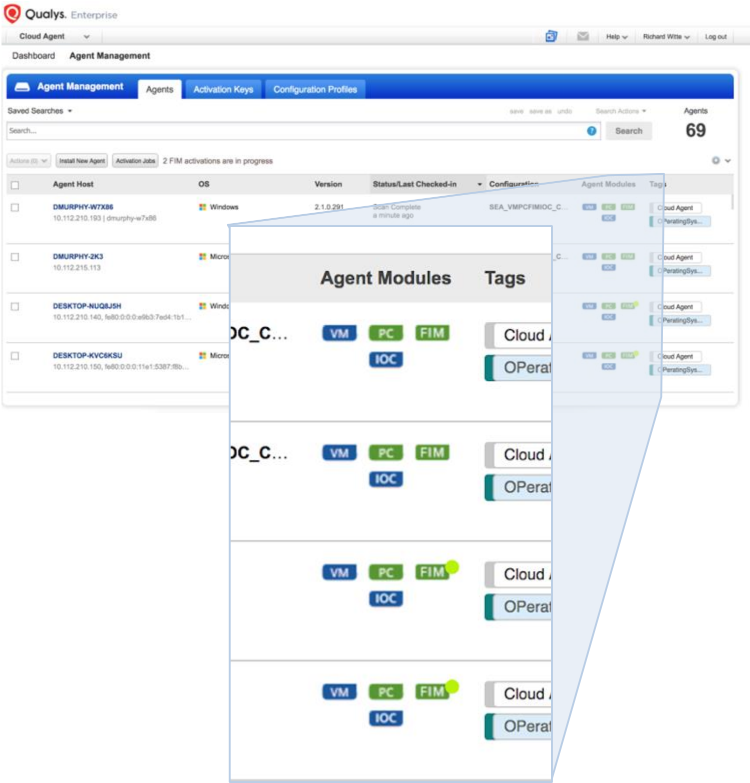
Delivers
Multiple
Built-in
Security
Functions in
one Agent

Qualys Cloud Agent

IT, Security, and Compliance Apps

Delivered by a single agent

- AI Asset Inventory
- VM Vulnerability Management
- PC Policy Compliance
- IOC Indication of Compromise Detection
- FIM File Integrity Monitoring
- PM Patch Management



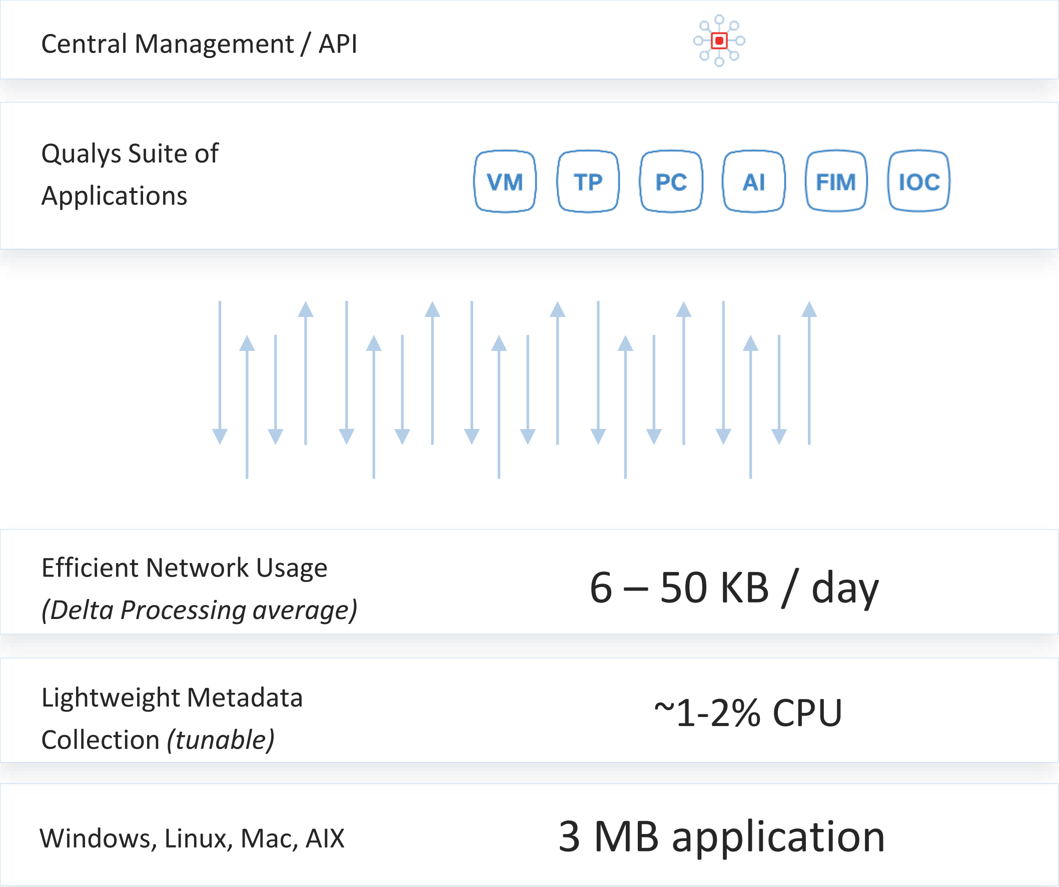
Agents 69

2 FIM activations are in progress

☐	Agent Host	OS	Version	Status/Last Checked-in	Configuration	Agent Modules	Tags
☐	DMURPHY-W7X86 10.112.210.193 | dmurphy-w7x86	Windows	2.1.0.291	Scan Complete a minute ago	SEA_VMPCFIMIOC_C...	VM PC FIM IOC	Cloud Agent OPeratingSys...
☐	DMURPHY-2K3 10.112.215.113	Micro			C...	VM PC FIM IOC	Cloud Agent OPeratingSys...
☐	DESKTOP-NUQ8J5H 10.112.210.140, fe80:0:0:0:e9b3:7ed4:1b1...	Windo				VM PC FIM IOC	Cloud Agent OPeratingSys...
☐	DESKTOP-KVC6KSU 10.112.210.150, fe80:0:0:0:11e1:5387:f8b...	Micro				VM PC FIM IOC	Cloud Agent OPeratingSys...

Qualys Platform

Cloud Agent



Central Management / API

Qualys Suite of Applications

Efficient Network Usage *(Delta Processing average)*

6 – 50 KB / day

Lightweight Metadata Collection *(tunable)*

~1-2% CPU

Windows, Linux, Mac, AIX

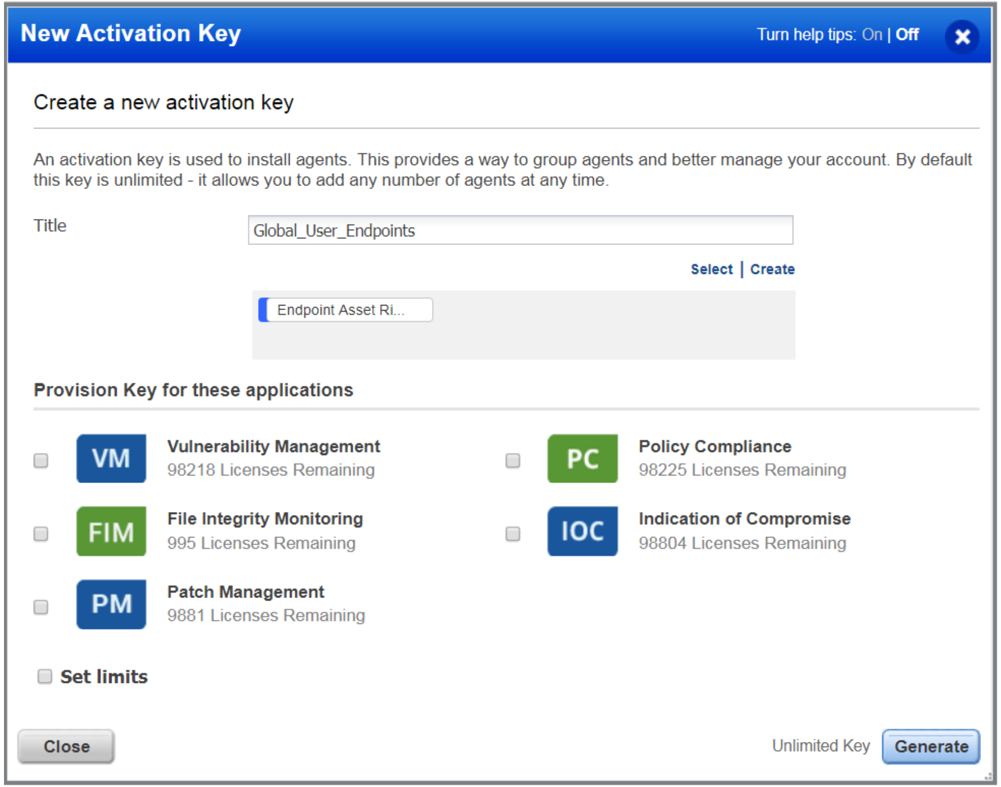
3 MB application

Deploy and Manage Apps on One Cloud Agent

End the fight with IT to deploy security agents!

Enabling an application does not require redeployment or reboot of the system

Self-updating, version control, elastic lifecycle management



New Activation Key

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Global_User_Endpoints

Endpoint Asset Ri...

Provision Key for these applications

- □ VM **Vulnerability Management** 98218 Licenses Remaining
- □ PC **Policy Compliance** 98225 Licenses Remaining
- □ FIM **File Integrity Monitoring** 995 Licenses Remaining
- □ IOC **Indication of Compromise** 98804 Licenses Remaining
- □ PM **Patch Management** 9881 Licenses Remaining

□ **Set limits**

Unlimited Key

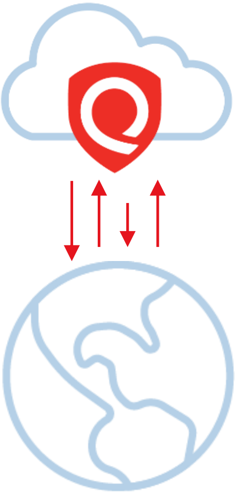
Cloud Agent Extends Network Scanning

No scan windows needed – always collecting

Find vulnerabilities faster

Detect a fixed vulnerability faster

Many new Apps only available on Agent



Best for assets that can’t be scanned

Unable to get credentials / authentication failures

Remote systems in branch offices / NAT

Roaming user endpoints

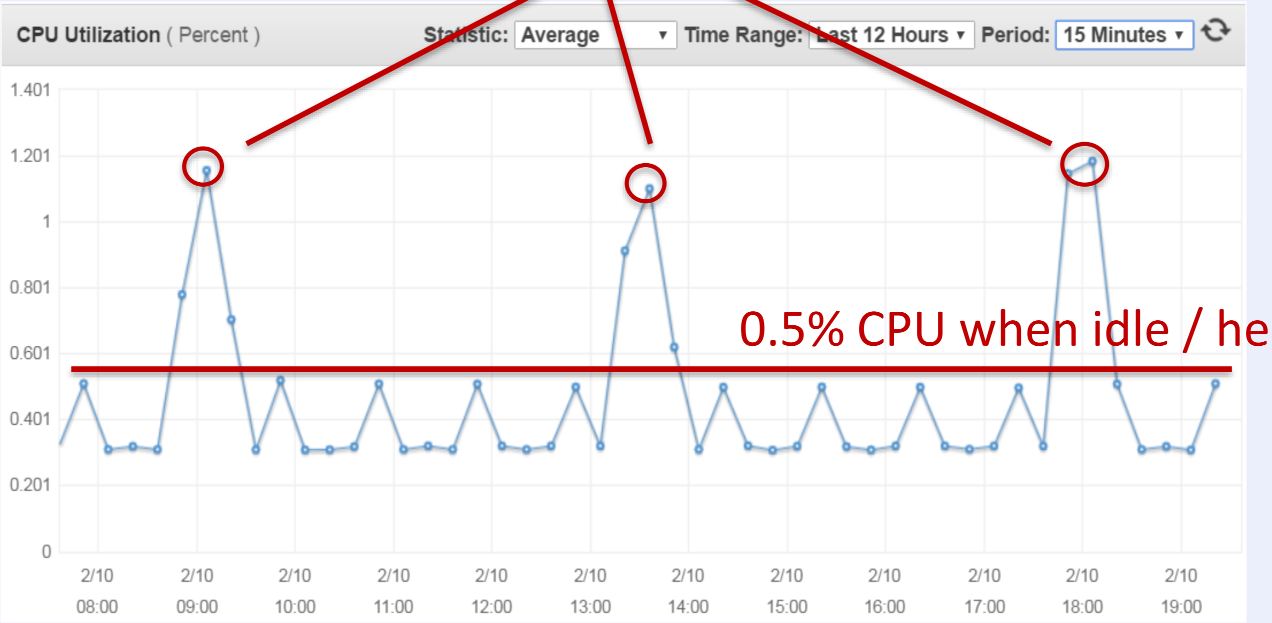
Cloud / Elastic deployments

Cloud Agent CPU Tuning - Linux

AWS EC2

not allowed to scan **nano, micro, or small instances** using network scanning

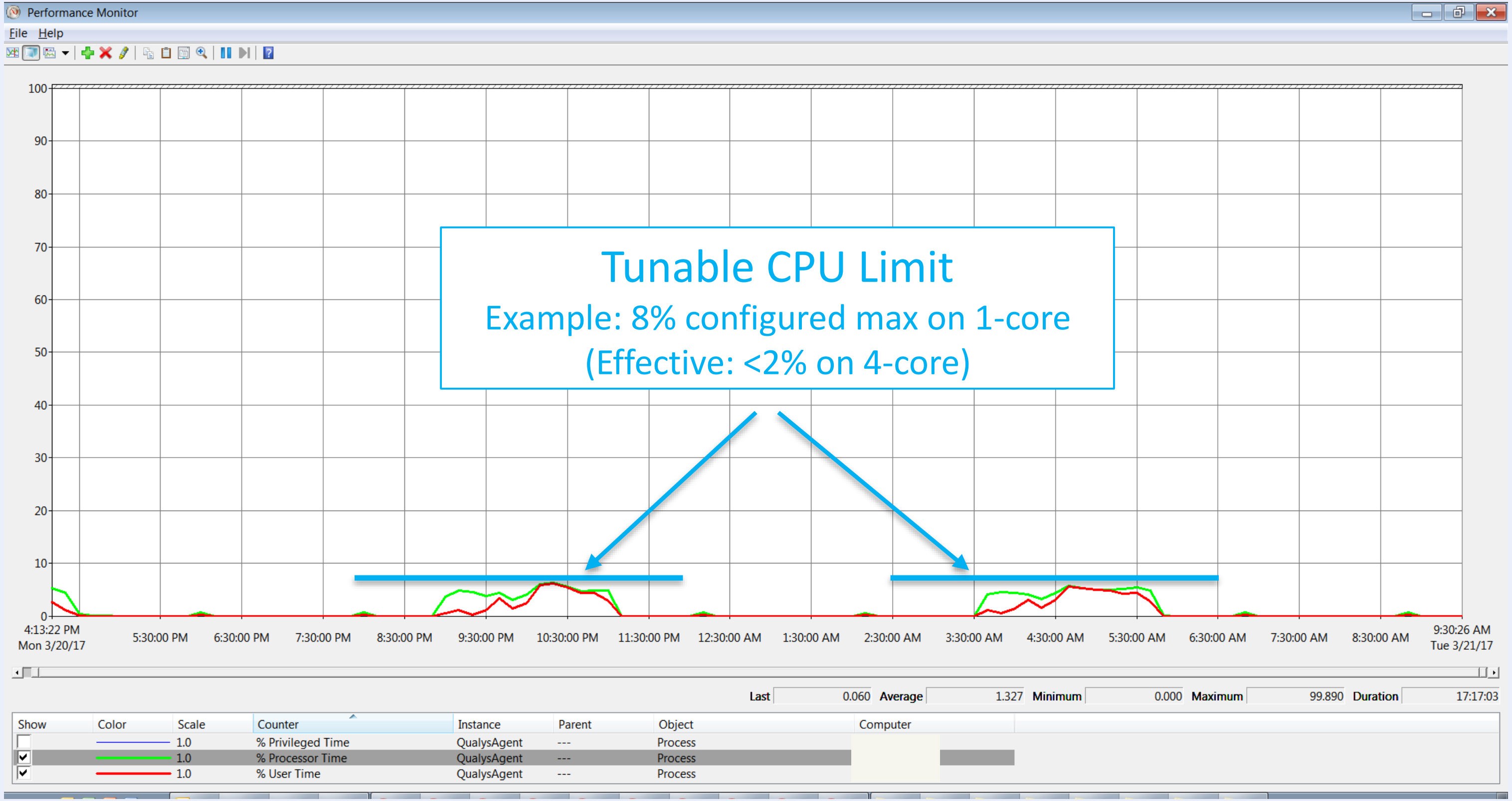
VM: < 1.2% CPU peak usage for less than 15 mins



0.5% CPU when idle / heartbeat

AWS t2.micro instance running Cloud Agent

Cloud Agent CPU Tuning - Windows



Tunable CPU Limit

Example: 8% configured max on 1-core

(Effective: <2% on 4-core)

Last	0.060	Average	1.327	Minimum	0.000	Maximum	99.890	Duration	17:17:03

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☐	🟦	1.0	% Privileged Time	QualysAgent	---	Process	
☑	🟩	1.0	% Processor Time	QualysAgent	---	Process	
☑	🟥	1.0	% User Time	QualysAgent	---	Process	

Cloud Native – Collect Provider Metadata

AWS EC2	Microsoft Azure	Google Compute Platform	IBM Cloud
accountId	dnsservers	hostname	
amiId	ipv6	**instanceId**	**Coming June 2019**
availabilityZone	location	macAddress	
hostname	macAddress	machineType	datacenterId
hostnamePublic	name	network	deviceName
instanceId	offer	privateIpAddress	publicIp
instanceType	osType	projectId	privateIp
kernelId	privateIpAddress	projectIdNo	**id**
macAddress	publicIpAddress	publicIpAddress	publicVlan
privateIpAddress	publisher	zone	domain
publicIpAddress	resourceGroupName		privateVlan
region	tags		
reservationId	subnet		
securityGroupIds	subscriptionId		
securityGroups	version		
subnetId	**vmId**		
VPCId	vmSize		

Agent collects metadata locally without Connector

2019 Cloud Agent Application Roadmap

Cloud App	Q1 Released	Q2	Q3	Q4
Patch Management	General Availability		Linux	Mac
Vulnerability Management				Middleware Auto-Discovery
Policy Compliance	User Defined Controls		Middleware Auto-Discovery Scan by Policy	Remediation
Indication of Compromise		Threat Feed Alerts/Actions	Linux	Mac Network IOCs
Asset Inventory			Detect Unmanaged Assets on the Network	

Roadmap schedule subject to change

Announcing

Cloud Agent Gateway

Available Now on Shared Platforms

Cloud Agent Deployment Questions

#1

I am not able to run Cloud Agent on assets that do not have direct access to the Internet due to security policies

#2

I am (A) not able to use existing proxies deployed by IT or (B) are not able to buy/manage an open-source or full-fledged commercial proxy

#3

I wish to optimize the bandwidth utilized by large Cloud Agents deployments and Patch Management

Qualys Cloud Agent Gateway (CAG)

A Qualys-developed HTTP proxy/cache running on a new virtual appliance platform

- Separate appliance from the Virtual Scanner

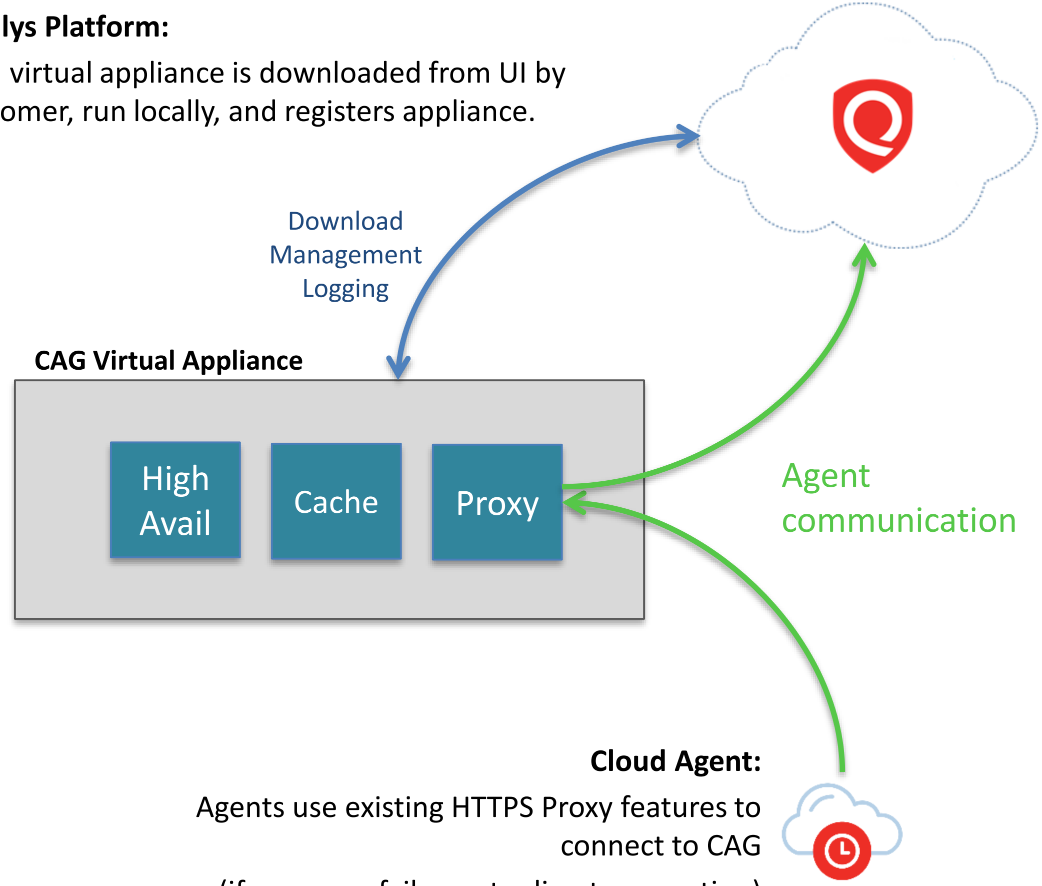
CAG appliances are downloaded and managed from Qualys Platform UI

Cloud Agents use existing agent proxy capabilities to connect through CAG to connect to the Qualys platform

How it works

Qualys Platform:

CAG virtual appliance is downloaded from UI by customer, run locally, and registers appliance.



Cloud Agent Gateway (CAG):

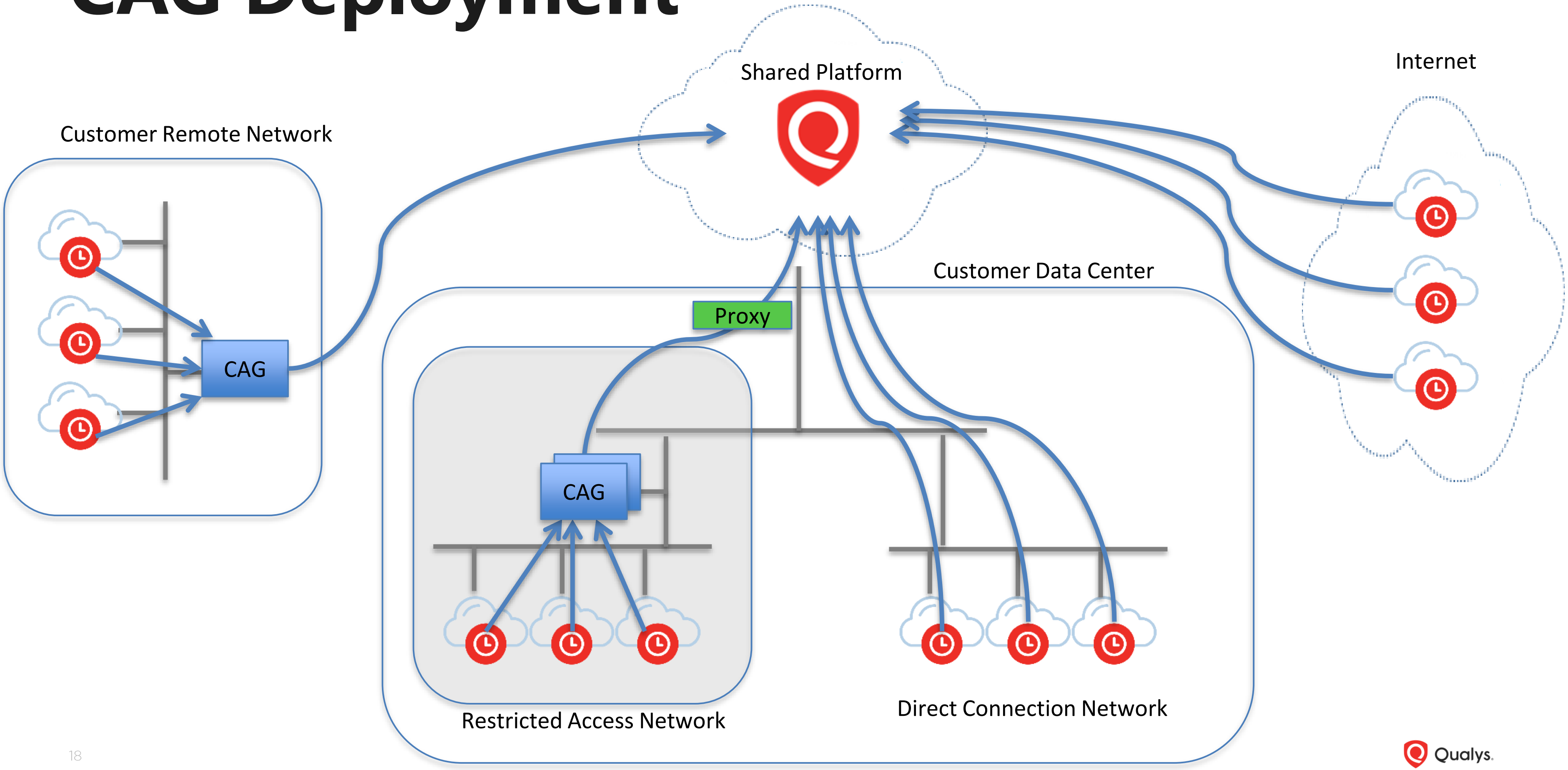
Virtual appliance with Docker containers providing HTTPS Proxying, Caching, Load Balancing, High-Availability, and Logging.

Cloud Agent:

Agents use existing HTTPS Proxy features to connect to CAG

(if no proxy, fail over to direct connection)

CAG Deployment



Expanded CAG Use Cases

Proxy/caching for Patch Management patch downloads

- Recommended/Required for on-premises agents

Thank You

Chris Carlson

ccarlson@qualys.com

Qualys Indication of Compromise

Bringing IOC to the Next Level

Chris Carlson
VP, Product Management, Qualys, Inc.

Adversary TTPs are Changing

Early 2010s

Zero-day Vulnerabilities

(Nation State, Industrial Espionage, Black Market)

Today

Rapidly weaponizing newly-disclosed vulnerabilities

(Lesser Nation State, Industrial, Organized Crime)

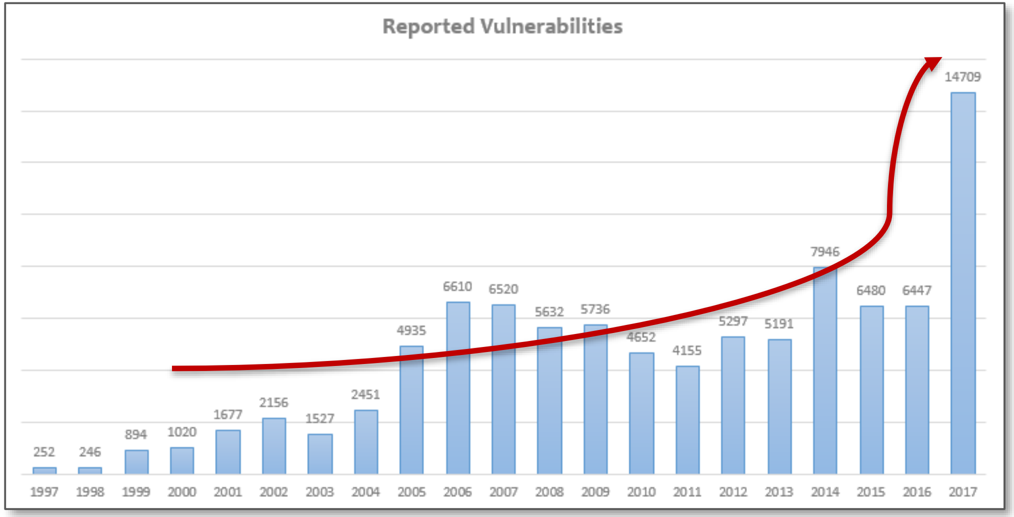
Good, Fast, Cheap – Pick all 3

Known Critical Vulnerabilities are Increasing

6-7K vulnerabilities are disclosed each year*

30-40% are ranked as “High” or “Critical” severity

“Mean Time to Weaponize” (MTTW) is rapidly decreasing y/y



Adversaries are Evading Anti-Virus Detection

Multiple Symantec Products CVE-2018-12238 Local Security Bypass Vulnerability

Bugtraq ID: 105917

CVE: CVE-2018-12238

Remote: No Local: Yes

Published: Nov 28 2018 12:00AM

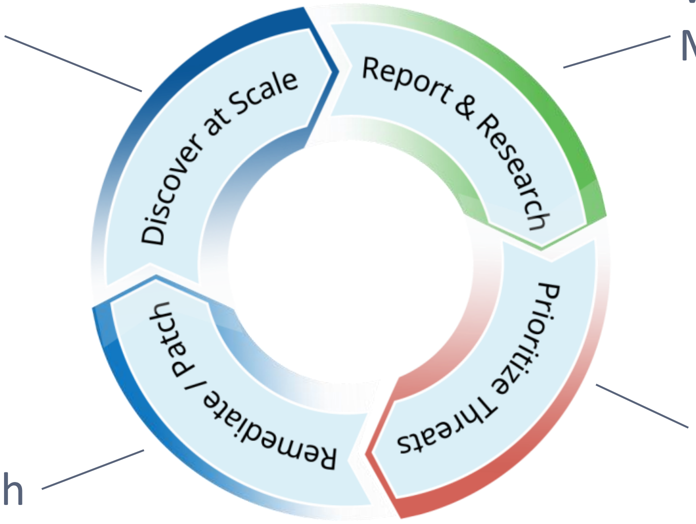
Credit: Qualys Malware Research Lab

Vulnerable:

Symantec Norton AntiVirus 22.7
Symantec Norton AntiVirus 21.0
Symantec Norton AntiVirus 17.6.0.32
Symantec Endpoint Protection Cloud 12.1.6
Symantec Endpoint Protection Cloud 14
Symantec Endpoint Protection 12.1.6 MP4
Symantec Endpoint Protection 12.1.6
+ 95 other products

QID 371337
QID 371338

Vulnerability Management Lifecycle



Asset Inventory

Vulnerability Management

Threat Risk and Prioritization

Patch Management

Get Proactive – Reduce the Attack Surface

Immediately Identify Vulnerabilities in Production

Notify IT Asset Owner to Patch/Stop the Instance

Change Configuration to Limit Access (Policy Compliance)

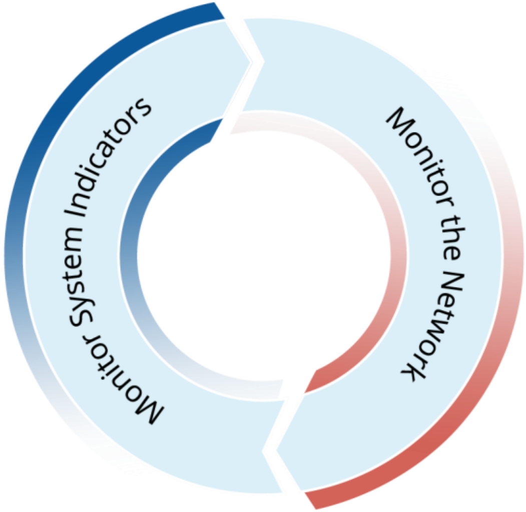
Control Network Access / Cloud Security Groups

Add Detection and Response – Endpoint & Network

Proactively Hunt, Detect, and Respond

Indication of Compromise

Detect IOCs, IOAs, and verify Threat Intel



Passive Network Sensor

What new devices are on the network? Are there new/different traffic patterns?

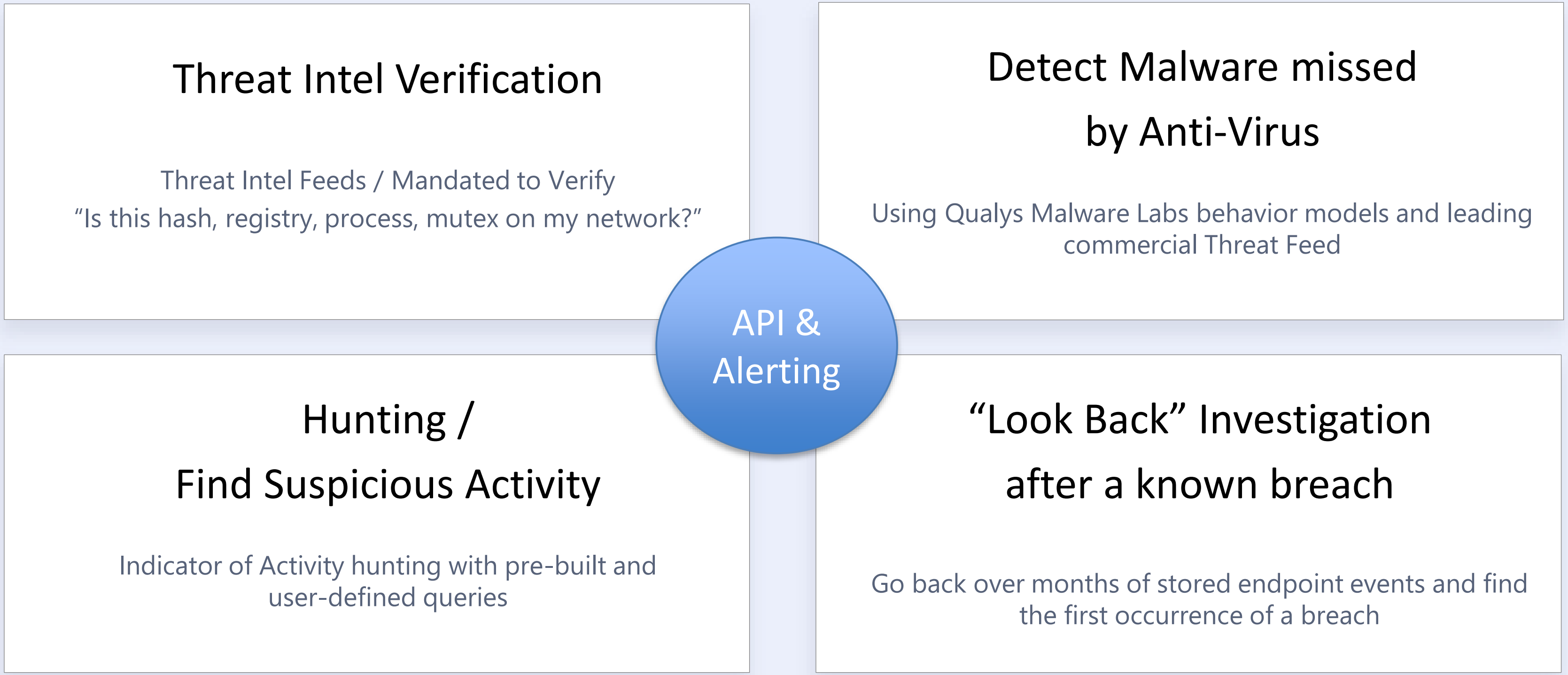
Organizations Struggle to Answer Basic Threat Questions

Are these hashes on/running in my network?
Or these mutexes / processes / registry keys?

Did any endpoints connect to these IPs / Domains?
Are there any connections to TOR exit nodes?

What system is the first impacted? *"Patient Zero"*
Did this spread to others systems? When?

Qualys IOC – Visibility Beyond Anti-Virus



Threat Intel Verification

Threat Intel Feeds / Mandated to Verify
“Is this hash, registry, process, mutex on my network?”

Detect Malware missed by Anti-Virus

Using Qualys Malware Labs behavior models and leading commercial Threat Feed

API & Alerting

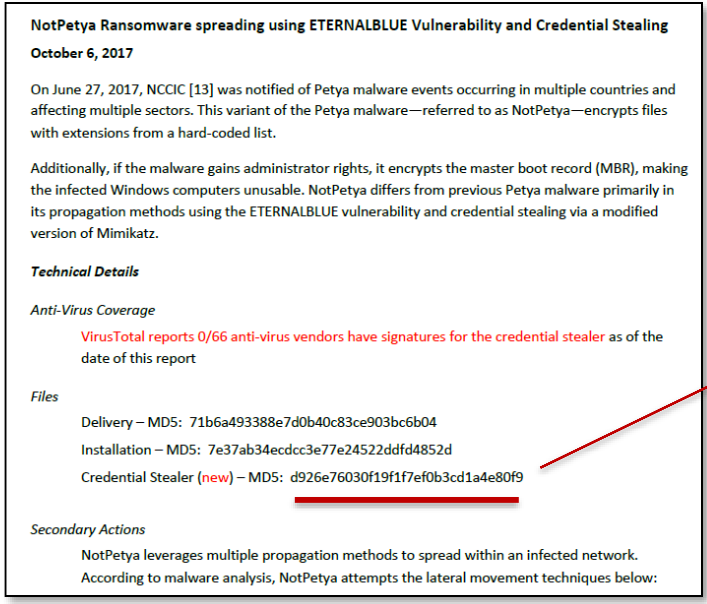
Hunting / Find Suspicious Activity

Indicator of Activity hunting with pre-built and user-defined queries

“Look Back” Investigation after a known breach

Go back over months of stored endpoint events and find the first occurrence of a breach

Threat Intel Verification



NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing

October 6, 2017

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.

Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.

Technical Details

Anti-Virus Coverage

VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report

Files

Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04

Installation – MD5: 7e37ab34ecdcc3e77e24522ddfd4852d

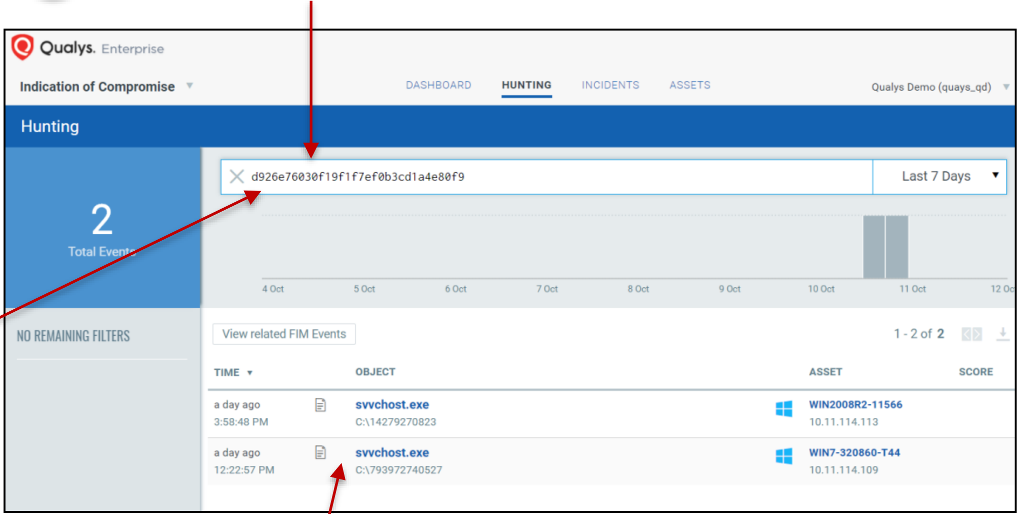
Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9

Secondary Actions

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

1 Threat Intelligence lists attack information …

2 Search for the file hash here…



d926e76030f19f1f7ef0b3cd1a4e80f9 | Last 7 Days

TIME	OBJECT	ASSET	SCORE
a day ago 3:58:48 PM	svvchost.exe C:\14279270823	WIN2008R2-11566 10.11.114.113	
a day ago 12:22:57 PM	svvchost.exe C:\793972740527	WIN7-320860-T44 10.11.114.109	

3 Find the object there.

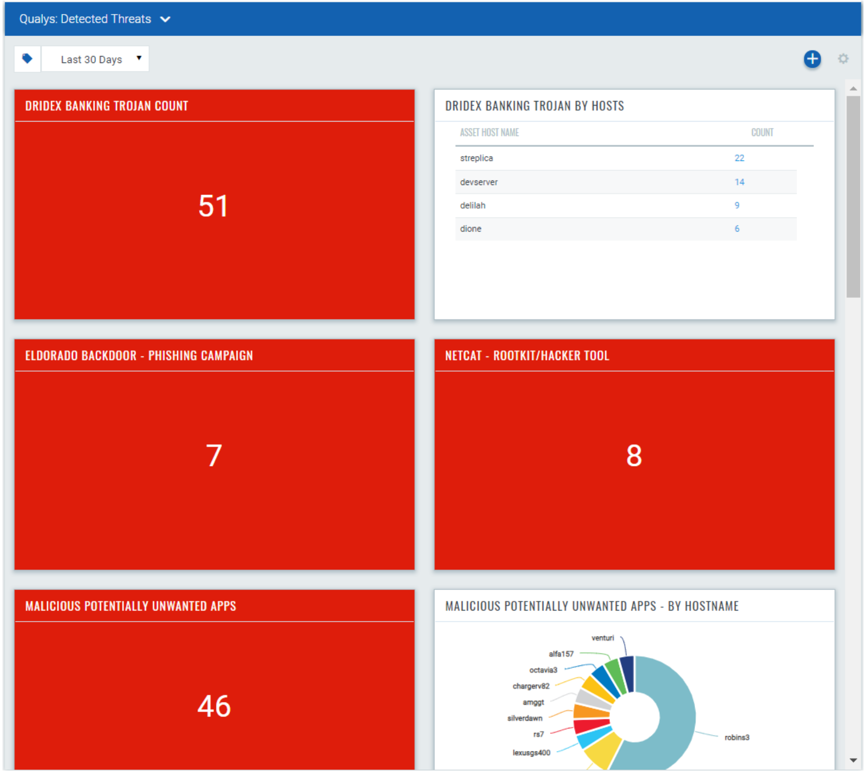
Detect Malware Missed by Anti-Virus

UK Government Contractor

- “Big 4” Anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents

Qualys IOC discovered…

- Dridex Banking Trojan (51)
- 4 Domain Controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed



Qualys: Detected Threats

Last 30 Days

DRIDEX BANKING TROJAN COUNT

51

DRIDEX BANKING TROJAN BY HOSTS

ASSET HOST NAME	COUNT
streplica	22
devserver	14
delilah	9
dione	6

ELDORADO BACKDOOR - PHISHING CAMPAIGN

7

NETCAT - ROOTKIT/HACKER TOOL

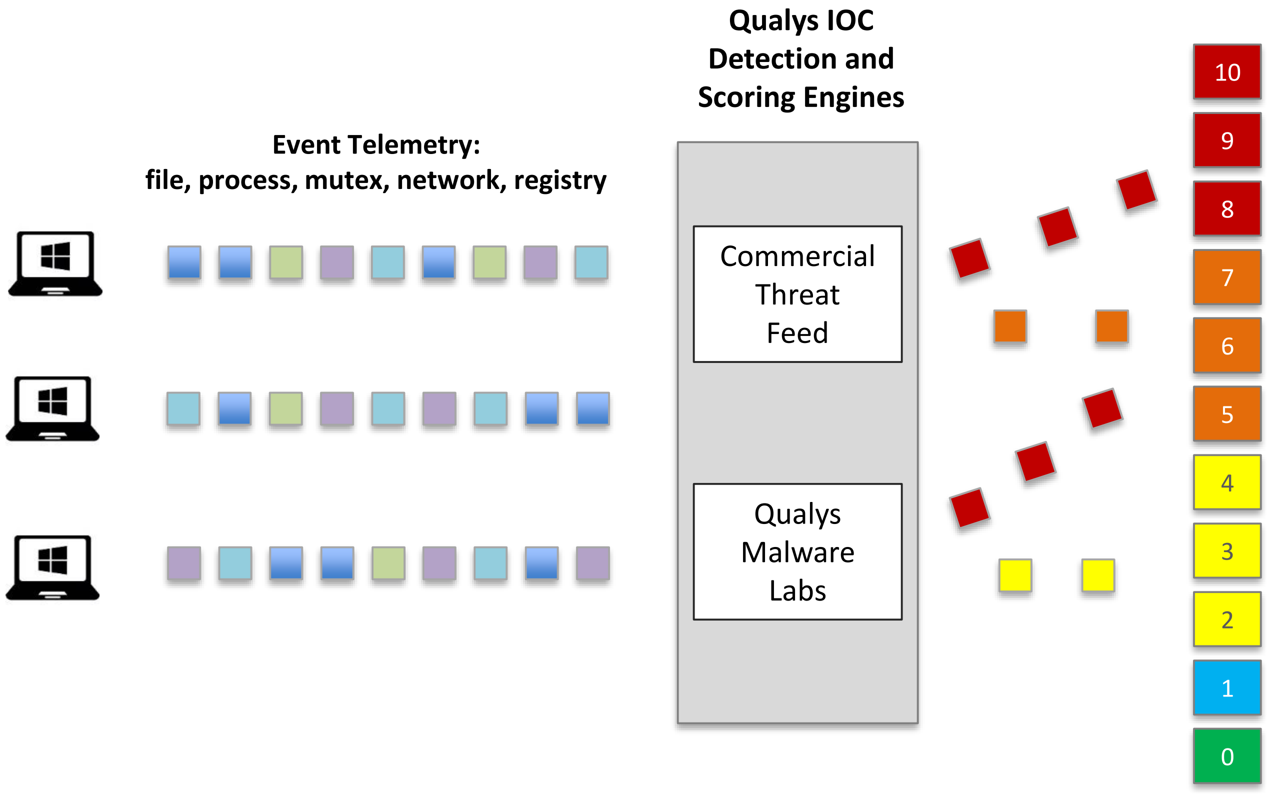
8

MALICIOUS POTENTIALLY UNWANTED APPS

46

MALICIOUS POTENTIALLY UNWANTED APPS - BY HOSTNAME

Malware Detection & Scoring – Actionable Responses



Event Telemetry:
file, process, mutex, network, registry

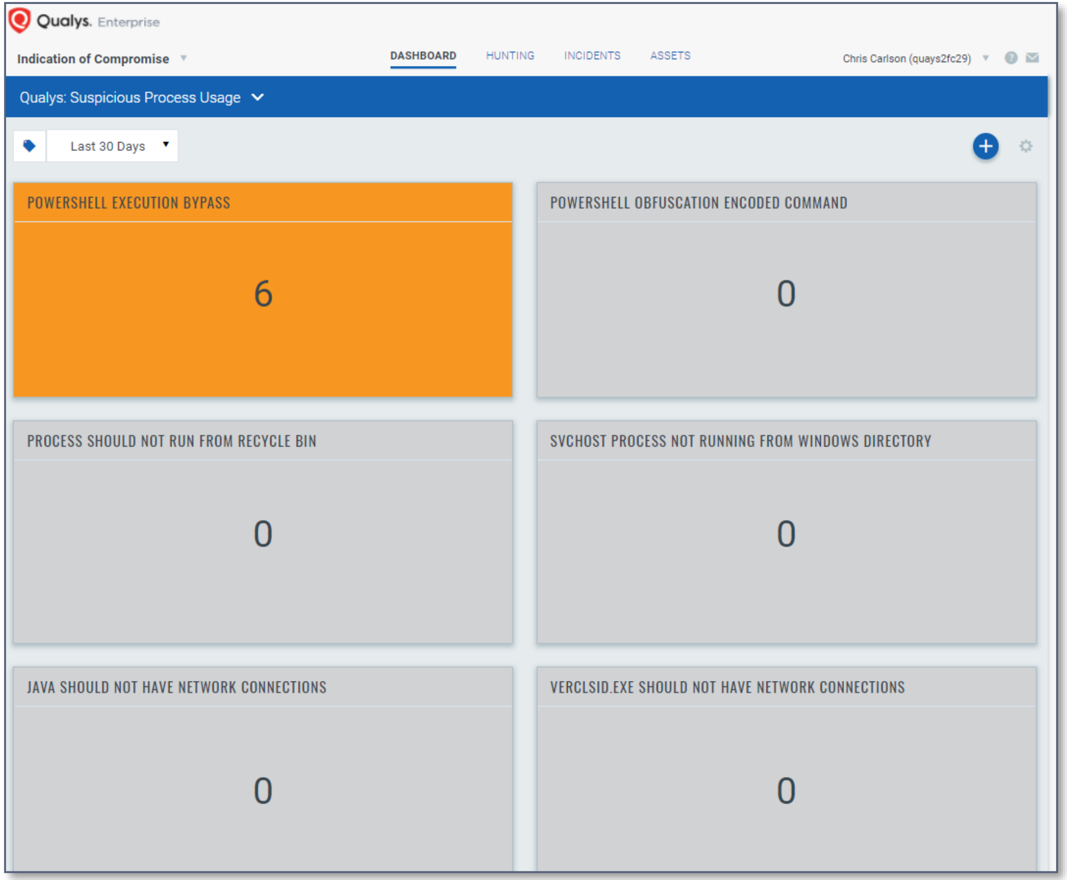
Qualys IOC Detection and Scoring Engines

Commercial Threat Feed

Qualys Malware Labs

Score	Description
10	**Confirmed** – Malicious Process w/ Network Connection
9	**Confirmed** – Malicious Process
8	**Confirmed** – Malicious File
7	**Medium Confidence** Suspicious – Process w/ Network Connection
6	**Medium Confidence** Suspicious – Process
5	**Medium Confidence** Suspicious – File
4	**Low Confidence** Suspicious – Process w/ Network Connection
3	**Low Confidence** Suspicious – Process
2	**Low Confidence** Suspicious – File
1	**Remediated** – Indicator no longer present
0	**Known Good**

Pre-Defined & Ad Hoc Threat Hunting



POWERSHELL EXECUTION BYPASS

6

POWERSHELL OBFUSCATION ENCODED COMMAND

0

PROCESS SHOULD NOT RUN FROM RECYCLE BIN

0

SVCHOST PROCESS NOT RUNNING FROM WINDOWS DIRECTORY

0

JAVA SHOULD NOT HAVE NETWORK CONNECTIONS

0

VERCLSID.EXE SHOULD NOT HAVE NETWORK CONNECTIONS

0

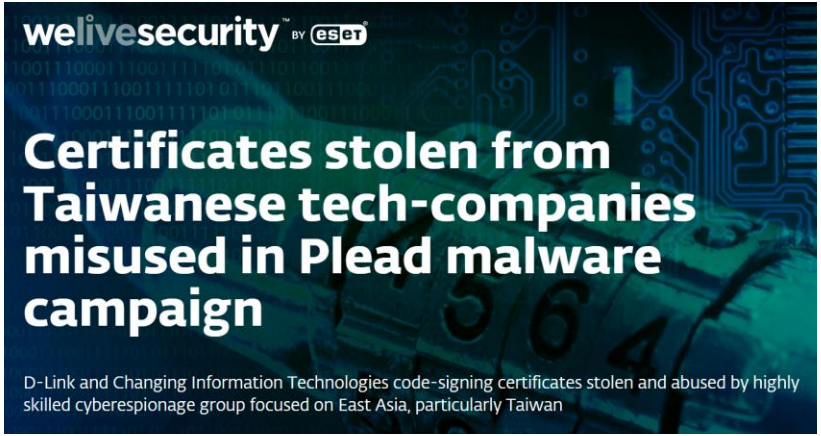
Suspicious process analysis to detect:

- “Fileless” malware attacks
- Non-malware attacks
- Malware evasion techniques
- Compromised processes

Find Malware using Stolen Code-Signing Certificates

July 2018

Certificates stolen from D-Link and others used by cyberespionage group



welivesecurity BY eset

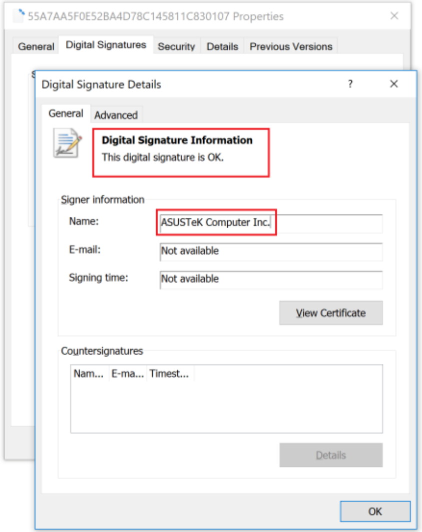
Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign

D-Link and Changing Information Technologies code-signing certificates stolen and abused by highly skilled cyberespionage group focused on East Asia, particularly Taiwan

https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

March 2019

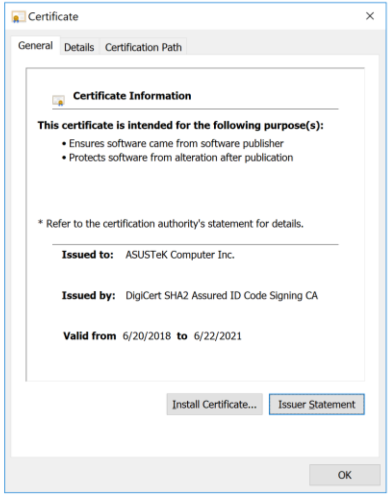
Hackers dropped a secret backdoor in Asus' update software



Digital Signature Information
This digital signature is OK.

Signer information
Name: ASUSTeK Computer Inc.
E-mail: Not available
Signing time: Not available

Countersignatures



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

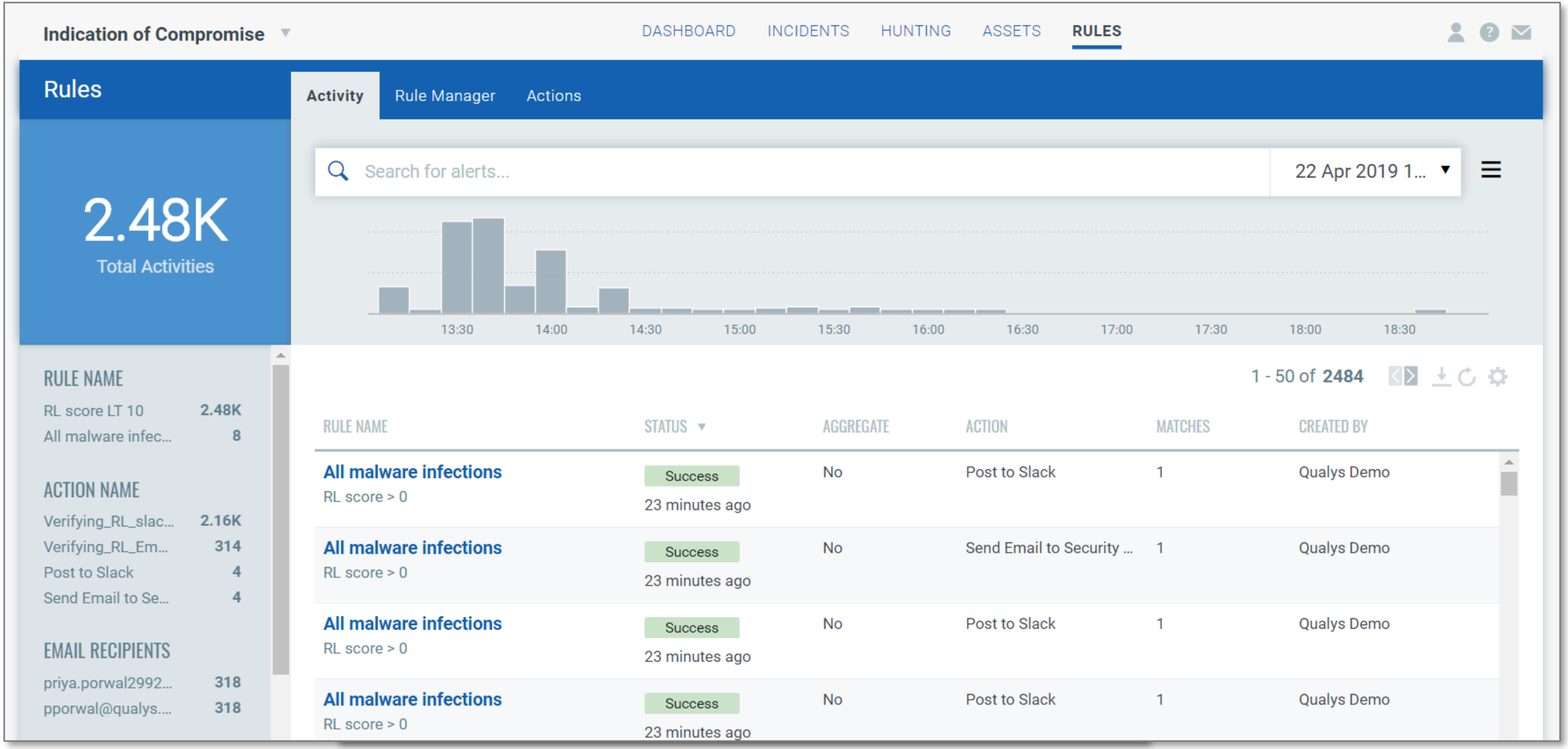
Issued to: ASUSTeK Computer Inc.

Issued by: DigiCert SHA2 Assured ID Code Signing CA

Valid from 6/20/2018 to 6/22/2021

https://techcrunch.com/2019/03/25/asus-update-backdoor/

Real-Time Responses – Rules, Search, Widgets



2.48K
Total Activities

RULE NAME	
RL score LT 10	2.48K
All malware infec...	8

ACTION NAME	
Verifying_RL_slac...	2.16K
Verifying_RL_Em...	314
Post to Slack	4
Send Email to Se...	4

EMAIL RECIPIENTS	
priya.porwal2992...	318
pporwal@qualys....	318

1 - 50 of **2484**

RULE NAME	STATUS ▼	AGGREGATE	ACTION	MATCHES	CREATED BY
All malware infections RL score > 0	Success 23 minutes ago	No	Post to Slack	1	Qualys Demo
All malware infections RL score > 0	Success 23 minutes ago	No	Send Email to Security ...	1	Qualys Demo
All malware infections RL score > 0	Success 23 minutes ago	No	Post to Slack	1	Qualys Demo
All malware infections RL score > 0	Success 23 minutes ago	No	Post to Slack	1	Qualys Demo

IOC

DEMO

Indication of Compromise

Threat Intel Verification / Hunting

Malware Detection

Alerting

5fda1d49ad9e08035b3893796191aff7e1dab06079e2e50ff1dc13911c33aee5

Thank You

Chris Carlson
ccarlson@qualys.com